International Journal of Electrical and Computing Engineering
Vol. 1, Issue. 1, July – 2014 *ISSN (Online): XXXX-XXXX*

Novel Detection Technique for Node Replication Attack in Mobile Sensor Network

Dr. BABUKARUPPIAH[1], JEYALAKSHMI.V[2], PRADEEPA.N[3], VINOTHA.R[4]

[1]Assistant Professor, [2,3,4] Under Graduates of Electronics and Communication Engineering
Velammal College of Engineering and Technology Madurai

***ABSTRACT*- A Wireless Sensor Network (WSN) consists of a number of ultra small, autonomous and resource-constrained sensor nodes, but is often deployed in unattended and harsh environments to perform various monitoring tasks. The WSN is vulnerable to security threats and susceptible to physical capture. Thus, it is necessary to use effective mechanisms to protect the network. This paper considers a typical threat in the latter category known as the node replication attack, where an adversary prepares own low-cost sensor nodes and deceives the network into accepting them as legitimate ones. The technique used in static networks to find the replicated nodes cannot apply to the mobile sensor networks because the location of the node is not stable in a network. Only few techniques are proposed for mobile sensor networks. In existing method to detect node replication attack many beacon signal are sent which is costly and not accurate .In this paper replicated nodes are detected by cluster head using their velocity by encryption and decryption techniques. The advantages of our proposed algorithm include 1) Accuracy 2) Efficiency 3) Reduces energy Consumption.**

1. INTRODUCTION

A. *Wireless Sensor Networks*

The Wireless sensor network is built of nodes from a few to several hundreds or even thousands, where each node is connected to one or sometimes several sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

B. *Security Attacks in Wireless Sensor Network*

The WSN has many different types of attacks

Flooding attack: Flooding attack is a type of denial of service attack in which the attacker send a large number of packets to the target node their by discontinues their communication in the network.

Jamming attack: In jamming attack, an electromagnetic interference is caused in the frequency of the network operations and also in the targeted receiver so that the transmitted message is corrupted.

Replay Attack: A replay attack is caused when the transmitted data is maliciously replayed. It is caused either by the originated. The forwarded packets are copied and repeatedly transmitted to the targeted node by the attacker

Spoofing Attack: in spoofing attack, the routing loop is created and the routing information are attracted and replayed so as to complicate the network by the adversary.

Sinkhole Attack: In the sinkhole attack, the base station is prevented from getting the information regarding the sensing data. It draws the attention of the network traffic by just advertising them as the trusted node or as the shortest path.

C. *Node Replication Attack*

Node replication attack is also known as clone attack. It exists in both the static and mobile Wireless sensor network. It creates an extensive harm to the network because the replicated node also has the same identity as the legitimate member. It is difficult to detect the replicated node in mobile sensor network since the location can vary from time to time. Node replication is done by adversary by compromising one sensor node and fabricates many replicas having the same identity from the captured node.

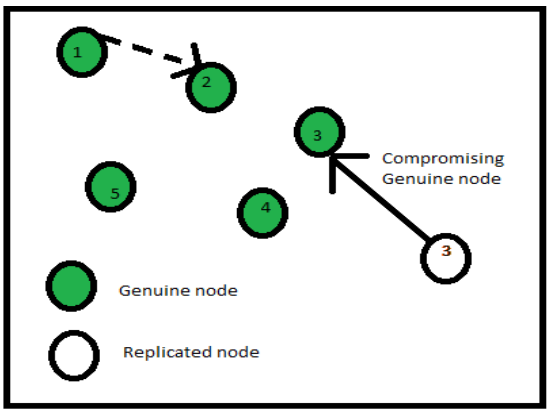


Fig 1.1 Node replication attack

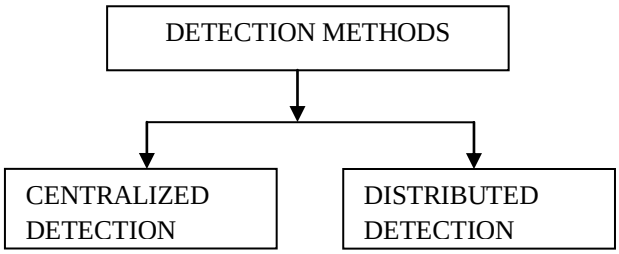
Fig 1.1 show the node replication attack where the attacker collecting information from genuine node to create a low cost replicated node

It is desirable but very challenging to have efficient and effective distributed algorithms for detecting replicas in mobile sensor network.

D. *Related Works*

In mobile sensor networks many works are existing for node replication attack. In those papers they had discussed about the 1) Witness finding strategy 2) Setting threshold value 3) Detecting the nodes with same identity [1], which consume more energy, time and accuracy is less it cannot find the replicated node but it will identify the replicated and genuine node. So the data for both the node will be blocked. They send both the location and the signature ({L (v), sig (L (v))} where L (v) is the location of v, sig (L (v)) is the signature of v) to their neighbouring nodes which consume more energy and time to detect the replicated node. Sometimes the replication is not found in large networks. Clusters are formed only for stationary network [11] which will be more efficient for mobile sensor network. They found the replication only in a particular range [16] which cannot be used in mobile sensor network. A threshold value is set for all nodes to communicate with each other but some time the genuine node may have the necessary to communicate above the threshold so the accuracy is less [2].The witness-finding strategy exploits the fact that one sensor node cannot appear at different locations, but, unfortunately, the sensor nodes in mobile sensor networks have the possibility of appearing at different locations at different times, so the schemes in static wireless sensor networks cannot be directly applied to mobile sensor networks. Slight modification of these schemes can be helpful for applicability to mobile sensor networks. For instance, the witness-finding strategy can adapt to mobile environments if a timestamp is associated with each location claim. In addition, setting a fixed time window in advance and performing the witness-finding strategy for every units of time can also keep witness-finding feasible in mobile sensor networks. Nevertheless, accurate time synchronization among all the nodes in the network is necessary. Moreover, when witness-finding is applied to mobile sensor networks, routing the message to the witnesses incurs even higher communication cost. After identifying the replicas, a message used to revoke the replicas, possibly issued by the base station or the witness that detects the replicas, is usually flooded throughout the network. Nevertheless, network-wide broadcast is highly energy consuming and, therefore, should be avoided in the protocol design. Time synchronization is needed. Nevertheless, it is still a challenging task to synchronize the time of nodes in the network, even though loose time synchronization is sufficient for the detection purpose. Hence, as we know that time synchronization algorithms currently need to be performed periodically to synchronize the time of each node in the network, thereby incurring tremendous overhead, it would be desirable to remove this requirement. Witness-finding could be categorized as a strategy of cooper active detection; sensor nodes collaborate in certain ways to determine which ones are the replicas. In this regard, the effectiveness of witness-finding could be reduced when a large number of sensor nodes have been compromised, because the compromised nodes can block the message issued by the nodes near the replicas. Hence, the witness nodes cannot discover the existence of replicas. The effectiveness in detecting replicas, all of the schemes adopting witness-finding have the common drawback that the detection period cannot be determined. In other words, the replica detection algorithm can be triggered to identify the replicas only after the network anomaly has been noticed by the network planner. Therefore, a detection algorithm that can always automatically detect the replica is desirable. Since the existing algorithms are built upon several other requirements, we have found that the common weakness of the existing protocols in detecting node replication attacks is that a large amount of communication cost is still unavoidable [1].

The node replication attack in mobile sensor nodes are detected by two methods



1. Centralized Detection

In mobile sensor networks there is only one centralized detection method called Sequential Probability Ratio Test (SPRT).

1.1 **Sequential Probability Ratio Test:** In SPRT [3], each and every time the node claims its location and time information to their neighbours and they forward it to the base station when they enter into a new location.

1.2 **Straight Forward Scheme:** In straight forward scheme [4] each node has to send a list of its neighbours and the positions claimed by these neighbours to the base station, which then examines every neighbour list to look for replicated sensor nodes. In a stationary WSN, conflicting position claims for one node id indicates a replication. Once the base station spots one or more

replicas, it can revoke the replicated nodes by flooding the network with an authenticated revocation message.

1.3 **Fingerprint Verification:** This scheme consists of two phases [6]. In the first phase, each node u computes for each neighbour v ϵ N (u) the fingerprint FPv, which is a reflection of v's fixed neighbourhood characteristics; node v itself is also capable of computing FPv. In the second phase, the legitimacy of the originator for each message is verified by checking the enclosed fingerprint, and the detection is conducted both ''at the sensor side'' (seemingly in a distributed manner by the notion) and at the base station. However, even the detection ''at the sensor side'' needs the base station to process the alarms for decision making, and thus the scheme is throughout centralized.

1.4 **Detecting Cloned Keys:** It assumptions and application scenarios are quit different from other approaches in fact it addresses the detection of cloned cryptographic keys rather than cloned sensor nodes and falls into the category of anomaly detection [2]. The basic idea is that in the context of random key pre-distribution the keys employed by genuine nodes should follow a certain pattern. Therefore it is possible to monitor the key usage as authentication tokens and then detect statistical deviations that indicate clone attack. the approach detects the cloned keys by node authentication statistics those keys whose usage exceeds a certain threshold are considered cloned and erased from the network.

1.5 **Set operation:** SET logically partitions[11] the network into non overlapping regions respectively managed by leaders, and has these leaders respectively report to the base station all the ids of the nodes in the region, in the form of the subset. Intuitively, the "Intersection" of any two subsets of reports should be empty; otherwise, replication is detected

2. *Distributed Detection*

There are two distributed detection methods they are eXtremely Efficient Detection (XED) and Efficient and Distributed Detection (EDD) [1]

2.1 **Extremely Efficient Detection:** XED has two steps Offline and Online step

2.1.1 **Offline Step:** It has a security parameter b and a cryptographic hash function h(.) are stored in each node. Two arrays of length n which keep the received random number and the materials used to check the legitimacy of received random number.

Two arrays are initialized to zero vectors.

B (u) - Initialized to be empty.

2.1.2 **Online step:** When two nodes u & v meet for first time it exchanges a random number. When v attempts to communicate with u next time, v should send the random number given by u during first meet. Then u check the random number given by v if the verification fails v will be blacklisted by u. If verification is success communication will be extended between u & v.

The effectiveness of XED, unfortunately, heavily relies on the assumption that the replicas do not collude with each other. When replicas can communicate with each other, the replica can always share the newest received random numbers with the other neighbouring replicas, thus degrading the detection capability because multiple replicas are able to reply with the correct random number to encountered genuine nodes accordingly.

2.2 **Efficient and Distributed Detection**: EDD has two steps offline and online steps

2.2.1 **Offline step:** In the network without replicas, the number of times a node meets a specific node should be limited for a given time interval.

2.2.2 **Online step:** In the network with replicas, the number of times a node meets a particular node should be greater than the threshold.

Since the effectiveness of EDD relies on the fact that each node faithfully and periodically broadcasts its ID, a strategy called selective silence could be taken by the replicas to compromise the detection capability of EDD.

3. PROPOSED WORK

Assumed that sensor network consist of n node with node ID {1, 2, 3..., n}.The nodes are assumed to move with a constant velocity for a particular distance and then remain stationary for specified time. More over the nodes are assumed to communicate only during stationary period. The nodes are allowed to move randomly. The network is divided into clusters which are monitored by the respective cluster head. The cluster head maintain the data base which contain node ID, velocity and key for each node. The initial velocity of each node is encrypted with a key and stored as a packet in that particular node. Whenever a node enters into a cluster it should send its node id to the cluster head. This paper consists of two scenarios.

1. Replication inside a cluster
2. Replication in different cluster

3.1 **Replication inside a cluster:** when a node enter into a cluster it should give its id to the cluster head the cluster head will check for the reputation of that id in that cluster if there is some other node inside that particular cluster then the cluster will send a packet to those two node with the same id. That packet asks for the encrypted velocity from

those two nodes. The node will send the packet with the encrypted velocity when this packet reach the cluster head it will decrypt the packet and check the velocity with its database. The node with different velocity is identified as replicated node. The request from replicated node is avoided and the replication is broadcasted to all cluster heads. So the replicated node cannot get any information from the network.

Fig 3.1 shows the replication inside the cluster. The data base has the velocity as V1 for node 1 so the request from new node is denied.

Node	1	2	3	4
Velocity	V1	V2	V3	V4

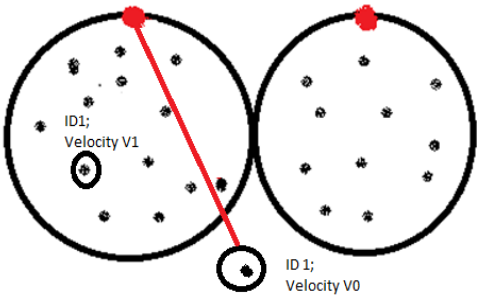


Fig 3.1 Node Replication Inside A Cluster

3.2 **Replication in different cluster: :** when a node enter into a cluster it should give its id to the cluster head the cluster head will check for the reputation of that id in that cluster if there is some other node inside that particular cluster. When there is no reputation in the same cluster the particular cluster head will intersect the data base of other cluster head to identify reputation. If there is reputation the cluster will send a packet to those two node with the same id. That packet asks for the encrypted velocity from those two nodes. The node will send the packet with the encrypted velocity when this packet reach the cluster head it will decrypt the packet and check the velocity by intersecting the database. The node with different velocity is identified as replicated node. The request from replicated node is avoided and the replication is broadcasted to all cluster heads. So the replicated node cannot get any information from the network.

Node	1	2	3	4	5
Velocity	V1	V2	V3	V4	V5

Node	1	6	7	8	9
Velocity	V0	V6	V7	V8	V9

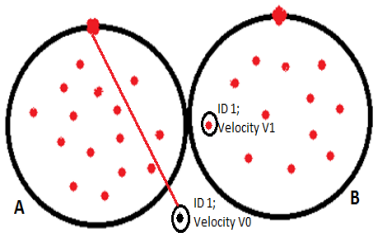


Fig 3.2 Node Replication On Different Cluster

Fig 3.2 Show the replication in different cluster. The Node with id 1 send request to the cluster A. The cluster A does not have any node with node id 1 so it intersect the database with other clusters the cluster head B has a node with node id 1. After verification the request from replicated node is denied

4. SIMULATION RESULTS

The proposed work is implemented using Network Simulator 2.The proposed work increased the energy efficiency and reduces the packet drop. In the existing work node id and location are broadcasted to neighbours and when a node get same id with different location it is found to be replicated with take more energy and time. To overcome this proposed work formed clusters with a cluster head this increases the energy efficiency. When the neighbour nodes get the details it will take time to find the replication if the replicated node and genuine nodes are far away. In the proposed work cluster head alone used to find the replica the time taken is so less. When the replicated node enters a cluster its genuinely is identified so the packet drop is not found the packet is forwarded only to the genuine node. The accuracy of finding the replicated node is high.

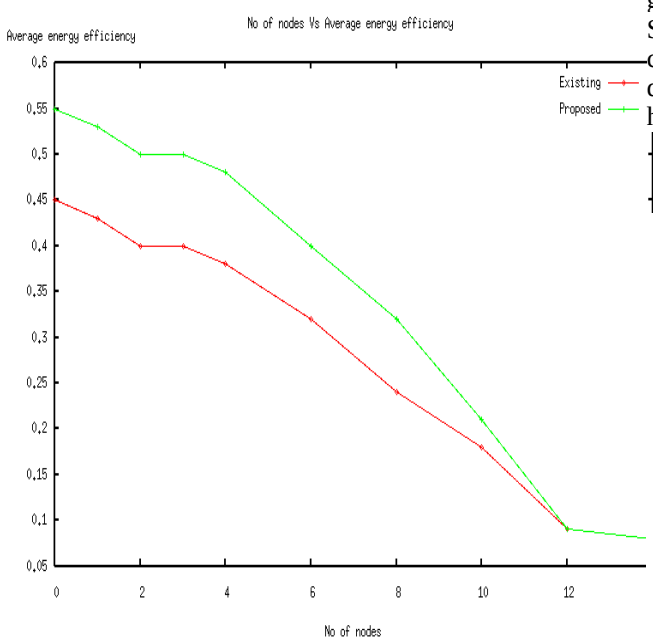


Fig 4.1 Energy Efficiency Graph

In the graph the X axis shows no of nodes and Y axis shows energy efficiency. Green line shows the energy efficiency of the proposed work and the red line shows the efficiency of existing method. When the number of node increase the efficiency goes down in existing work. In the proposed work the efficiency level is high compared with previous works. The increase in efficiency is due to the formation of cluster the node id is send only to cluster head in existing work the location and id is send to neighbours and the nodes are used to find the replication in the network.

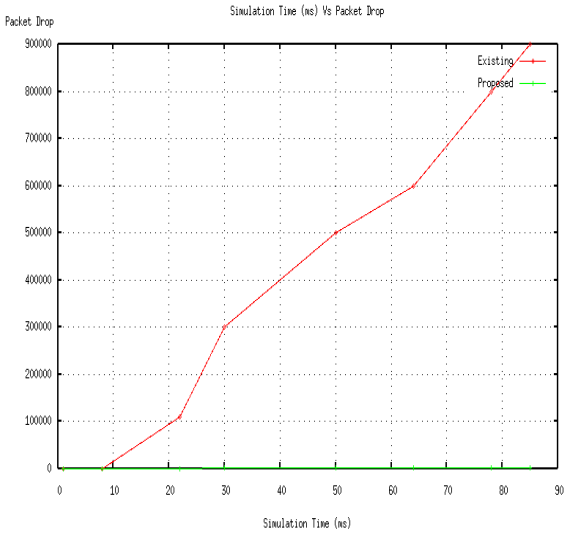


Fig 4.2 Packet Drop Graph

In the above graph the X axis shows the time and the Y axis shows the packet drop. The red line shows the packet drops in existing work and the green line shows the packet drop in proposed work. Since the nodes are verified before entering the cluster which avoid packet drop. As the packet drop become less the packet delivery ratio become high which is shown in the Fig 4.3

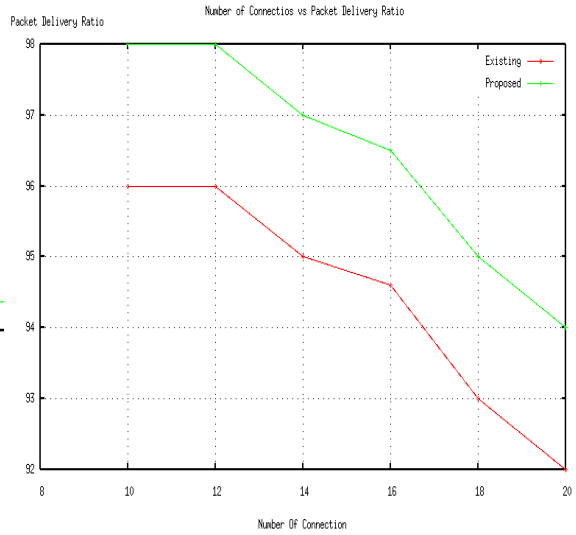


Fig 4.3 Packet Delivery Ratio Graph

In the graph X axis shows number of connection and Y axis shows packet delivery ratio. The green line shows the packet delivery ratio of proposed work and the red line shows the packet delivery ratio of existing work. The packet delivery ratio is high for the proposed work.

5. CONCLUSION

In the proposed work formation of cluster and detecting replication is the main work. In the first method replication inside the cluster alone is found in order to improve the accuracy second method is proposed which is used to find the replication in different cluster too. The proposed work increased the efficiency and accuracy in finding node replication attack.

REFERENCES

1. Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu, Member, IEEE, and Sy-Yen Kuo, on "Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Network" IEEE transactions on information forensics and security, vol. 8, no. 5, may 2013

2. R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the Detection of Clones in Sensor Networks using Random Key Predistribution," IEEE Trans. Syst., Man, Cybern. C, Ap- plicat. Rev., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

3. Ho J-W, Liu D, Wright M, Das SK. on "Distributed Detection of Replica Node Attacks with Group Deployment Knowledge in Wireless Sensor Networks, Ad Hoc Network" 2009;7(November): 1476-88.

4. Parno B, Perrig A, Gligor V.Distributed detection of node replication attacks in sensor networks In: proceedings of the 26th IEEE symposium on security and privacy;2005

5. Poovendran R, Wang C, Roy S. Secure Localization and Time Synchronization for Wireless Sensor and Ad hoc Networks.New York Inc: Springer-Verlag; 2007.

6. Xing K, Liu F, Cheng X, Du DHC, Real time detection of clone attacks in wireless sensor networks. In: proceedings of the 28th international conference on distributed computing systems 2008.

7. Li Z, Gong G. DHT-Based Detection of Node Clone in Wireless Sensor Networks. In:Proceedings of the 1st international conference on ad hoc networks (ADHOCNETS'09); 2009b. p. 240–55

8. Zhang Q, Yu T, Ning P. A framework for Identifying Compromised Nodes in Wireless Sensor Networks. ACM Transactions on Information and Systems Security 2008; 11(March): 12:1–37. September

9. Zhu WT, Zhou J, Deng R, Bao F. Detecting Node Replication Attacks in Mobile Sensor Networks: theory and approaches. Security and Communication Networks, available online May 2011.

10. Zhang M, Khanapure V, Chen S, Xiao X. Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Networks. In: Proceedings of the 17th IEEE international conference on network protocols (ICNP'09); 2009. p. 284–93. October

11. Wen Tao Zhu, Jianying, Robert H.Deng, FengBao on Detecting Node Replication Attacks in Wireless Sensor Networks Journal of network and computer application 35(2012)

12. C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Noninteractive pairwise key es- tablishment for sensor networks," IEEE Trans. Inf.Forensics Security, vol. 5, no. 3, pp. 556–569, Sep. 2010.

13. S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks," in Proc. IEEE Symp. Security and Privacy (S&P), Oakland, CA, USA, 2004, pp. 259–271.

14. D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996

15. J. Yi, J. Koo, and H. Cha, "A localization technique for mobile sensor networks using archived anchor information," in Proc. IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON), California, USA, 2008, pp. 64–72.

16. Huang Jian, Xiong Yan, Li Ming-Xi, Miao Fu You, "A Range- based detection method of replication attacks in wireless sensor networks". International Conference on Information and computer networks,2012.